## AMENDMENTS TO THE CLAIMS

The listing of claims will replace all prior versions, and listings, of claims in the application.

## Listing of Claims

Claims 1-4. (Cancelled)

5. (Previously Presented) A method for managing a log list, which is an issuing history of a digital signature issued on a message by a digital signature issue side apparatus, in a signature history storage service apparatus comprising:

accepting the log list from the digital signature issue side apparatus,

verifying validity of the digital signature of a digital signer signed on the log list or log list registration request data,

verifying consistency between the accepted log list and a registered log list of a registered digital signer,

adding and registering the accepted log list with the confirmed consistency to the registered log list of the digital signer, and

registering a user of the signature history storage service apparatus who is a digital signer of the digital signature issue side apparatus.

6. (Previously Presented) The method for managing a log list according to claim 5, further comprising:

confirming the consistency is confirmed, and

transmitting a fact that the accepted log list is added and registered to the registered log list of the digital signer, to a digital signer side apparatus.

7. (Previously Presented) The method for managing a log list according to claim 5 comprising:

a step in which the digital signature issue side apparatus requests registration of the accepted log list to the signature history storage service apparatus, and

a step in which log data other than the newest log data included in the accepted log list is deleted if the additional registration notice is received.

8. (Previously Presented) The method for managing a log list according to claim 7, wherein

the digital signature issue side apparatus performs:

a step comprising issuing electronic data of a deposition request document for indicating intention of a registration request, and

a step comprising transmitting the issued deposition request document electronic data, a public key certificate, and log list data, to the signature history storage service apparatus and

as the step for verifying the validity of the digital signature, the signature history storage service apparatus performs:

a step comprising verifying the validity of the received public key certificate, and

a step comprising checking whether or not the deposition request document is verified correctly by use of a public key of a user included in the public key certificate.

9. (Previously Presented) The method for managing a log list according to claim 7, wherein the digital signature issue side apparatus requests registration of the log list every time when a digital signature is issued.

Claims 10-19. (Cancelled)

20. (Previously Presented) The method of claim 5 for managing a log list, which is an issuing history of a digital signature issued on a message by a digital signature issue side apparatus, in a signature history storage service apparatus, further comprising:

sending an additional registration notice to the digital signature issue side apparatus after registering the accepted log list to the registered log list, and

deleting in the digital signature issue side apparatus log data other than the newest log data of the digital signer included in the accepted log list when the digital signature issue side apparatus receives the additional registration notice sent from the signature history storage service apparatus.

21. (Previously Presented) The method for managing a log list according to claim 20, wherein

the digital signature issue side apparatus performs:

a step comprising issuing electronic data of a deposition request document for indicating intention of a registration request, and

a step comprising transmitting the issued deposition request document electronic data, a public key certificate, and log list data, to the signature history storage service apparatus, and

the step for verifying the validity of the digital signature, the signature history storage service apparatus performs:

a step comprising verifying the validity of the received public key certificate, and

a step comprising checking whether or not the deposition request document is verified correctly by use of a public key of a user included in the public key certificate.

22. (Previously Presented) The method for managing a log list according to claim 20, wherein the digital signature issue side apparatus requests registration of the accepted log list every time when a digital signature is issued.

23. (Previously Presented) The method for managing a log list according to claim 20, wherein said verifying consistency is performed by calculating a hash value h (Rn') of the signature issuing record Rn', and confirming that the hash value h (Rn') in the signature issuing record Rn'+1 is identical with the calculated h (Rn').